

RECEIVED Attorney Docket No. 60097-0145
CENTRAL FAX CENTER

AUG 08 2006
REMARKS/ARGUMENTS

I. STATUS OF CLAIMS

Claims 1-28 remain in this application.

II. CLAIM REJECTIONS – 35 U.S.C. § 102

The Final Office Action rejected Claims 1-28 as being clearly anticipated by Vicard (U.S. Patent No. 5,764,761). The rejection is respectfully traversed.

Applicant notes that the Office Action cites elements of Claims 1 and 14 incompletely. The Office Action cites specific claim elements in Claims 1 and 14 as follows:

Claim 1:

“generating a response value using a combination of a lock value at said second party”

Claim 14:

“means for generating a response value using a combination of a lock value at said second party”

However, the actual elements for Claims 1 and 14 appear as follows (emphasis added):

Claim 1:

“generating a response value using a combination of a lock value **and said challenge value** at said second party”

Claim 14:

Attorney Docket No. 60097-0145

“means for generating a response value using a combination of a lock value and said challenge value at said second party”

Therefore, the Office Action has omitted portions of the claim elements of Claims 1 and 14.

Claims 1 and 14 appear as follows:

1. A computer implemented method for providing access between a first party and a second party, said method comprising the steps of:
 - generating a challenge value at said first party;
 - transmitting said challenge value to said second party;
 - generating a response value using a combination of a lock value and said challenge value at said second party;
 - wherein said lock value indicates a desired access mode;
 - transmitting said response value to said first party; and
 - validating said response value by said first party.
14. An apparatus for providing access between a first party and a second party, said apparatus comprising:
 - means for generating a challenge value at said first party;
 - means for transmitting said challenge value to said second party;
 - means for generating a response value using a combination of a lock value and said challenge value at said second party;
 - wherein said lock value indicates a desired access mode;
 - means for transmitting said response value to said first party; and
 - means for validating said response value by said first party.

In particular, in the Response to Arguments section of the Office Action, the Office Action equates Vicard's chip to a first device. The Office Action states:

“... Vicard discloses a first device (Chip) that is provided with a lock circuitry that controls operational enablement of a functional block of the chip. The

Attorney Docket No. 60097-0145

lock circuitry inhibits operation of the device until the response value of the second device is matched with the challenge value and lock value.”

However, Vicard does not teach or disclose the interaction between a first party and a second party as claimed in Claims 1 and 14. Claim 1 cites:

“generating a challenge value at said first party;
transmitting said challenge value to said second party;”

Vicard clearly shows in col. 3, lines 8-35 and Fig. 1 that Vicard’s chip 10 does not generate a challenge value nor does it transmit a challenge value to a second party. In fact, Vicard’s chip 10 only receives a chip-key from an external source (i.e., second device as described in the Office Action). Col. 3, lines 21-35 describe how a chip-key is received by chip 10 via communication block 20 and is used to unlock lock circuitry 11 and enable block 12, both of which reside in chip 10. The chip-key is decrypted and processed through a one-way function and then compared to a signature stored in a register. Upon a successful comparison, an external clock signal is gated through lock circuitry 11 to block 12 (col. 3, line 39-col. 4, line 2). This clearly shows that Vicard’s chip 10 only receives a chip-key and in no way generates a challenge value and transmits the challenge value to a second party.

It is unclear why the Office Action points to col. 3, lines 8-20 to demonstrate the generation of a challenge value when col. 3, lines 8-20 describe a gating circuit within chip 10 that gates an external clock signal from control line 17 to line 16 that enables block 12 that is also within chip 10. This operation has nothing to do with the generation of a challenge value nor does it have anything to do with transmitting the challenge value to a second party.

It is also unclear why the Office Action, in the Response to Arguments section, equates Vicard’s chip-key output as the claimed challenge value and Vicard’s chip-key signature derived from the one-way function as the claimed response value. These functions

Attorney Docket No. 60097-0145

on the chip-key are performed internally by the lock circuitry 11 that is contained within chip 10. The chip-key is received by chip 10 from an external source. Chip 10 does not create or store the chip-key and transmit it to a second party because chip 10 only knows the signature of the correct chip-key. Since the chip 10 only knows the signature of the correct chip-key, it cannot know what the actual chip-key value is and further cannot transmit the chip-key value to a second party. Vicard teaches away from the possibility of chip 10 knowing the chip-key value by teaching that a copy of the chip-key is not stored on the chip 10 to ensure confidentiality (col. 3, lines 39-41) and it is not computationally feasible to gain access to the chip-key signature in register 25 and determine the chip-key value (col. 3, lines 50-54). Therefore, the Office Action's equating of the chip-key value to the challenge value is illogical.

Even if chip 10 knew the chip-key value, it makes no sense that chip 10 would transmit the chip-key to anyone because that would be a breach of security. Therefore, it is illogical that the chip-key or even the chip-key output is the challenge value as the Office Action states.

The Office Action also equates the chip-key signature as the response value. However, the one-way function that creates the chip-key signature is internal to chip 10 (the first device as indicated by the Office Action) and therefore cannot be generated by a second party. Additionally, the chip-key signature cannot be a response value that is generated by a second party using a challenge value (generated by a first party) and a lock value. The chip-key signature is a result of the one-way function resident in chip 10 that operates on a chip-key. Since the chip-key signature is internal to chip 10, it could not be generated by a second party nor could it be transmitted to a first party.

Attorney Docket No. 60097-0145

Further, Vicard does not teach or disclose generating a response value using a combination of a lock value and said challenge value at said second party as claimed in Claims 1 and 14. The Office Action points to col. 3, lines 21-54 as showing such a feature. However, as discussed above, Vicard does not teach or disclose generating a challenge value at a first party and transmitting said challenge value to said second party. Since Vicard does not teach those elements, Vicard cannot teach generating a response value using a combination of a lock value and said challenge value at said second party because Vicard only addresses the internal workings of chip 10 which only receives a chip-key from an external source. Vicard does not address how a second party generates a response value using a combination of a lock value and a challenge value that was received from a first party. Therefore, Vicard does not contemplate such a feature.

Additionally, Vicard does not teach or disclose transmitting said response value to said first party as claimed in Claims 1 and 14. Since Vicard does not contemplate generating a challenge value at a first party and transmitting said challenge value to said second party and, further, generating a response value using a combination of a lock value and said challenge value at said second party, Vicard cannot teach transmitting said response value to said first party.

The Office Action points to col. 3, lines 40-55 as teaching transmitting said response value to said first party, however this is incorrect. As discussed above, Vicard teaches in col. 3, lines 40-55 that chip 10 ensures the confidentiality of the correct chip-key value by instead storing, in a register, a signature of the correct chip-key using a one-way function. This has nothing to do with transmitting said response value to said first party because Vicard does not contemplate how a response value is generated as cited in Claims 1 and 14, i.e., the response value is generated at said second party using a combination of a lock value

Attorney Docket No. 60097-0145

and said challenge value, where the challenge value is generated by the first party and transmitted to the second party. Once again, Vicard does not contemplate the interaction between the first party and the second party as cited in Claims 1 and 14.

Finally, Vicard does not teach or disclose wherein said lock value indicates a desired access mode as claimed in Claims 1 and 14. The Office Action points to col. 3, lines 21-54 as teaching such a feature. However, as discussed above, Vicard only teaches that chip 10 receives a chip-key. The chip-key can only be one value because it is compared to a signature of a correct chip-key (col. 3, line 39-col. 4, line 2). There is no possibility that Vicard's chip 10 could interpret a chip-key other than for unlocking block 12. Therefore, Vicard cannot contemplate that a lock value indicates a desired access mode because Vicard only has no access modes and can only unlock block 12.

Anticipation under 35 U.S.C. § 102 requires a reference to teach or disclose each and every element, limitation, or step of a claim. Since Claim 1 and Claim 14 each include at least one element not found in Vicard, the Vicard patent does not anticipate Claim 1 or Claim 14 under 35 U.S.C. § 102.

Vicard therefore does not teach every aspect of the claimed invention either explicitly or impliedly.

Claims 1 and 14 are allowable. Claims 2-13, and 15-28, are dependent upon independent Claims 1 and 14, respectively. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. 102(b).

III. MISCELLANEOUS

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

P0017

7

BEST AVAILABLE COPY

Attorney Docket No. 60097-0145

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments herein and further examination on the merits are respectfully requested.


The Examiner is invited to telephone the undersigned at (408) 414-1214 to discuss any issue that may advance prosecution.

No fee is believed to be due specifically in connection with this Reply. To the extent necessary, Applicants petition for an extension of time under 37 C.F.R. § 1.136. The Commissioner is authorized to charge any fee that may be due in connection with this Reply to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: August 8, 2006


Kirk D. Wong
Reg. No. 43,284

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 214
Facsimile No.: (408) 414-1076

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office Fax No. (571) 273-8300.

on August 8, 2006

by 

Annette Jacobs